Statement for the Record
R. James Caverly,
Director, Partnerships and Outreach Division,
Office of Infrastructure Protection, Department of Homeland Security
before the
Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee
of the Committee on Homeland Security
United States House of Representatives
July 26, 2007

Thank you Chairwoman Harman, Ranking Member Reichert, and Members of the Subcommittee. It is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS's) perspective on private-sector information sharing, specifically with the nation's Critical Infrastructure and Key Resources (CI/KR) stakeholders.

The challenge of protecting the nation's CI/KR is daunting. Human, physical, and cyber assets, systems, networks, and functions are spread across 17 critical infrastructure and key resource sectors, diverse in their composition, cultures, regulatory regimes, and operational processes. In aggregate, the CI/KR sectors represent almost 50 percent of the nation's Gross Domestic Product, with a majority of assets, systems, and networks owned and operated by the private sector. The protection of the nation's CI/KR represents a shared responsibility by owners, operators, and all levels of government through complementary commitment of resources, knowledge, and capabilities.

Building trust and effective working relationships with the private sector to facilitate information sharing is essential for effective CI/KR protection. The Sector Partnership model and other information-sharing mechanisms and tools described in the National Infrastructure Protection Plan (NIPP) provide the structure and processes within which public- and private-sector security partners share vital information to mitigate the nation's CI/KR risks.

The Challenge of Information Sharing

The NIPP defines the nation's CI/KR as "those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The wide scope of this definition of CI/KR underscores the wide variety in the 17 sectors' approaches to information sharing. Sectors differ in business characteristics and their sensitivity to risk taking; the assets, systems, networks, and functions involved; their previous experience in working with government; and the specific risk-management characteristics of the sector.

One factor that all CI/KR sectors have in common, however, is that in their public-private partnerships necessary for CI/KR protection, the desired outcome is a safer, more secure, and more resilient sector. Information sharing is effective when it clearly and directly supports this outcome.

Because information sharing is valued by both the CI/KR owners and operators and by the government, a collaborative approach enables public and private security partners to determine how best to apply their respective resources and capabilities to the entire spectrum of risk-management activities: prevention/deterrence; protective programs; preparedness; response and crisis management; and, recovery, restoration, and reconstitution.

Information Sharing and CI/KR Decision Making

Information sharing by both public- and private-sector security partners on threat trends, criticality (consequences), possible vulnerabilities based on emerging threats, protective priorities, best practices, and strategic solutions enables CI/KR risk management and must support several levels of decision making:

(1) Strategic planning and investments in preparedness and protective programs by both CI/KR owners and operators and government at all levels.

(2) Situational awareness and decision-making coordination during the execution of planned preparatory actions, protective measures, and response/recovery efforts.

(3) Operational/tactical decision making through the exchange of incident or suspicious activities information and the timely and accurate transmission of alerts and threats to CI/KR owners and operators to catalyze protective actions.

In the complex, dynamic environment that is characteristic of CI/KR-protection decision making, effective information sharing must be centered on clearly defined "knowledge networks" of public- and private-sector professionals and senior managers with the ability and authority to make decisions and act on critical, focused information. The bottom line for CI/KR information sharing is to get the right information to the right people who can make decisions and take the correct actions to protect the CI/KR and to mitigate consequences.

The Sector Partnership

The Sector Partnership model described in the NIPP is the foundation for effective information sharing with the owners and operators of facilities and systems in the CI/KR sectors. The scope of activities for CI/KR protection requires valid, two-way information sharing, which requires the trust that can only come with the implementation of a real partnership between the sectors and government. The Sector Partnership provides a national forum for requirements identification, planning and policy coordination, and the mutual path forward for implementation and operations for effective information sharing

among the CI/KR owners and operators, federal agencies, and state, local, and tribal government.

The components of the Sector Partnership provide the policy, planning, coordination, and implementation of CI/KR protection programs and its supporting information sharing environment. These components include the following.

Sector Coordinating Councils (SCCs) serve as the government's principal point of entry into each sector to address the entire range of CI/KR protection and risk-management issues. SCCs are self-organized, self-governing entities consisting of a broad base of sector infrastructure owner-operators and their representatives from sector trade associations. Often chaired by a sector owner-operator, SCCs serve as "honest brokers," facilitating sector-wide harmonization and coordination of the sector's CI/KR protection policy development, planning, program implementation, and monitoring activities. Each SCC identifies and supports the information-sharing mechanisms, needs, and capabilities most appropriate for its sector.

Government Coordinating Councils (GCCs) serve as the governmental counterparts to the SCCs. Each GCC is chaired by the Sector-Specific Agency (SSA) for the sector, as designated by Homeland Security Presidential Directive 7 (HSPD-7) and the NIPP, and includes representatives from DHS, the SSA, and other appropriate supporting government agencies. GCCs are non-regulatory in nature, are intended to maximize interagency coordination and information sharing at the operating level, and are tasked to institutionalize a true partnership with DHS and other government partners. GCCs provide coordinated communication, issue-development services, and initiative implementation among government partners. Each GCC engages and supports its corresponding SCC's efforts to plan, implement, and execute the necessary sector-wide measures for CI/KR protection, including information sharing within the government and with the sector.

The Partnership for Critical Infrastructure Security (PCIS) serves as the cross-sector council for the CI/KR owners and operators. It coordinates cross-sector initiatives in support of public and private efforts to promote assured and reliable provision of critical infrastructure services in the face of emerging risks to economic and national security. PCIS membership consists of one or more members and their alternates from each of the SCCs.

The Federal Senior Leadership Council (FSLC) is an interagency group that consists of senior representation from each SSA. The Council addresses common issues, dependencies, and impacts that cut across the sectors. The formation of the FSLC enhances communications and coordination among federal departments and agencies with a role in implementing the NIPP and HSPD-7.

The State Local Tribal Territorial Government Coordinating Council (SLTTGCC) serves as a forum to coordinate and communicate among state, local, and tribal homeland security advisors or their equivalents, and to ensure that they are fully integrated as active

participants in national CI/KR protection planning and implementation activities. With the implementation of the SLTTGCC, state, local, and tribal homeland security leadership can engage with the national security leadership of the CI/KR owners and operators and the federal government to identify and implement an effective framework for cooperation and coordination. The result can then be tailored for regional differences that will integrate the capabilities of national CI/KR protection programs with those implemented at the regional, state, or local level.

The Government Cross-Sector Council serves to coordinate government activity across sectors. It is made up of two sub-councils: the FSLC and the SLTTGCC.

Mechanisms for Policy and Strategy Coordination

Advisory committees are a way of ensuring public and expert involvement and advice in federal decision-making. The Critical Infrastructure Partnership Advisory Council and the National Infrastructure Advisory Council allow government and owner-operators to undertake collaboration and information sharing to support policy/strategy, planning, and requirements identification.

The Critical Infrastructure Partnership Advisory Council (CIPAC) membership consists of the CI/KR owners and operator members of all SCCs and their corresponding GCC organizations. It employs a special exemption (pursuant to Section 871 of the Homeland Security Act) to the Federal Advisory Committee Act. This exemption protects SCC and GCC discussions containing sensitive CI/KR information from public disclosure, thereby facilitating regular, ongoing, and multi-directional communications and coordination.

The National Infrastructure Advisory Council (NIAC) is the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. It comprises up to 30 CEO-level leaders from private industry and state and local government. The NIAC is charged with improving the cooperation and partnership between the public and private sectors in securing critical infrastructure and advising on policies and strategies that range from information sharing to roles and responsibilities between public and private sectors. In October 2005, the NIAC issued its recommendations for implementing the Sector Partnership, many of which were subsequently adopted by DHS. In addition, in July 2006, the NIAC issued recommendations regarding the Intelligence Community's coordination with CI/KR owners and operators. As a result of the collaboration between the Director of National Intelligence, the Program Manager of the Information Sharing Environment, the DHS Office of Intelligence and Analysis (OIA), and other members of the Intelligence Community, there have been significant advances toward meeting the intent of those recommendations.

Support Mechanisms

A series of operational mechanisms exists to support information sharing with the CI/KR sectors. These mechanisms consist of the organizations, processes, and personnel that support the exchange of information among DHS, other Federal agencies, State, local and tribal governments, and the CI/KR sectors. Efforts can be categorized into four broad areas

1. Content Development

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) is a partnership between OIA and the Office of Infrastructure Protection (OIP) within DHS. It provides tailored risk assessment products for CI/KR sectors, fusing consequence and vulnerability information from infrastructure protection communities collected through OIP with threat information from intelligence and law enforcement communities. It has access to a network of sector experts through the SSAs and SSCs, to specialists, and to field-deployed Protective Security Advisors to obtain CI/KR Sector expertise. Products include: 1) strategic risk assessments for each CI/KR sector; 2) threat handbooks; 3) information bulletins; and 4) analytic reports on suspicious-activity reports to sectors. Initial experience and feedback from the sectors using HITRAC products strongly indicate that it is a mechanism that delivers useful, actionable information.

Office of Infrastructure Protection Division, as a part of their CI/KR protection mission responsibility, this office develops information products on vulnerability, consequences, interdependencies, and protective strategies, as well as recommended effective practices. This information, combined with threat analysis provided through the Office of Intelligence and Analysis, results in information used by the CI/KR sectors.

The Sector Specific Agencies (SSAs) as mentioned above, are the Federal departments and/or agencies identified in HSPD-7 as responsible for CI/KR protection activities in specified CI/KR sectors. Along with other CI/KR relevant functional agencies**,** they bring expertise, authorities, experience, and content in participating as partners within the CI/KR information-sharing environment. Particularly in hazards risk management beyond terrorism, many SSAs have long traditions of working with their CI/KR sector counterparts, as well as deep-seated expertise**.** Consequently, they have information products useful to the CI/KR sectors. The SSAs are also fully engaged as partners in the development of the Homeland Security Information Network sites, which DHS has provided each of the sectors as an information-sharing tool.

2. Information Delivery Mechanisms

The National Infrastructure Coordination Center (NICC) is the round-the-clock watch mechanism through which the National Operations Center (NOC) maintains situational and operational awareness, communications, and coordination with CI/KR partners. It provides a centralized process for coordination and delivery of information between the government and the CI/KR sectors, particularly the SCCs, GCCs, and the

sector-based Information Sharing and Analysis Centers when they exist for a sector. The NICC serves as a DHS focal point for CI/KR suspicious activity and incident and status reporting; receives, logs, and tracks requests for information and assistance from the owners and operators of the CI/KR; and provides industry partners with Web-enabled access (via the Homeland Security Information Network) to DHS Situation Reports, bulletins, and other products. The NICC uses the Executive Notification System to provide rapid turn-around notifications of needed action, such as alerts and warnings.

The Homeland Security Information Network-Critical Sectors (HSIN-CS) is the primary technology tool to facilitate the information sharing necessary for coordination, planning, mitigation, and response. HSIN-CS is an Internet-based platform that enables secure, encrypted, Sensitive-But-Unclassified/For-Official-Use-Only-level communications between DHS and vetted members of the CI/KR sectors, as well as within and across the sectors. DHS fully funds and maintains HSIN-CS, thereby removing the obstacles of cost and day-to-day efforts required to support systems implementation, operations, and maintenance. DHS supports the unique requirements, outreach, and program-support needs of the CI/KR users to create robust, sector-specific information-sharing hubs for each sector. HSIN-CS includes a separate site for each CI/KR sector, designed and implemented in collaboration with the sector's GCC and SCC to best meet sector-specific needs. It also provides a top-level publishing capability to share applicable DHS and other information resources with all sectors simultaneously. HSIN-CS directly supports the building of trusted, reliable, and valued public-private sector partnerships, as well as two-way sharing of information.

Critical Infrastructure Warning Information Network (CWIN) provides a survivable network, not susceptible to service disruptions, to connect entities essential to restoring the nation's infrastructure during incidents of national significance. It connects key operational CI/KR sector entities, emergency operations centers of the 50 states, the District of Columbia, and the NOC.

3. Relationship Management

Sector-Specific Agencies (SSAs) As mentioned previously, the SSA's have the responsibility of working with each sector to implement the NIPP framework and guidance, as tailored to the sector's specific characterisitics and risk landscape. They serve as the key point of contact between the sector and the federal government to coordinate critical infrastructure protection, incident response, and infrastructure recovery.

Sector Specialists develop and sustain relationships at the national level with sector stakeholders to build trust and promote partnership. The Sector Specialist maintains extensive situational awareness of infrastructure issues and priorities. They keep a finger on the pulse of sector activities (economic, political, technological, and structural) to assess their implications on sector operations and security. The Sector Specialists are housed within the Office of Infrastructure Protection and HITRAC.

Protective Security Advisors provide field-deployed support to CI/KR owners and operators on specialized CI/KR security topics. They facilitate, coordinate, and/or perform vulnerability assessments in support of CI/KR owners and operators; they also assist with security efforts coordinated through state homeland security advisors, as requested.

4. Enabling Programs for CI/KR Information Sharing

The Protected Critical Infrastructure Information (PCII) Program provides a structure and processes to ensure that voluntarily submitted critical infrastructure information will be exempt from public disclosure, will not be used for regulatory purposes, and will be properly safeguarded. To implement and manage the program, DHS has created the PCII Program Office within the Infrastructure Partnerships Division in OIP. The PCII Program Office receives and evaluates critical infrastructure information to determine whether it qualifies for protection under PCII. The Office also manages a certification program for other Federal agencies and States to receive and manage PCII-protected information.

CI/KR Classified Security Clearance Program provides a capability whereby the federal government can discuss and share classified information – on vulnerability and consequences, as well as threats – with the owners and operators of the CI/KR. The owners and operators of the CI/KR will always have the primary responsibility for managing the risks of their own assets, systems, and functions. They also have current information on their operational and business processes, the usage and application of technology in their CI/KR sector, and what is most critical to their operations, including dependencies on other sectors and locality to locality variations. The Classified Security Clearance program is sponsored, coordinated, and funded by OIP. It is implemented through DHS's Office of Security and its policy and procedures framework.

CI/KR-Unique Policy and Legal Framework

For CI/KR owners and operators, sharing information with government at all levels creates a range of risks affecting the viability and efficiency of their business operations, including liability risk, antitrust risk, and competitive risk.

The risks associated with liability and competitiveness are the primary reasons that infrastructure owners and operators seek ownership and control over CI/KR data that they submit to government. They want to know who gets the information, what is done with it, and how is it protected from inappropriate disclosure. These assurances, to the extent possible, are necessary for building trust in government institutions and processes that receive and handle voluntarily submitted CI/KR information.

The Information-Sharing Environment

Our information-sharing efforts are part of the broader Information-Sharing Environment (ISE) created by the President in accordance with the Intelligence Reform and Terrorism

Prevention Act of 2004. The purpose of the ISE is to measurably improve information sharing between and among the Federal government, appropriate State, local, and tribal officials, and private-sector entities. In recognition of the important work under way in this area under the NIPP framework, the program manager for ISE, in coordination with the Information Sharing Council, has officially designated the CI/KR NIPP process (as described above) as the mechanism in which the private sector will be incorporated into the ISE. In this role, the NIPP Partnership Framework provides guidance for the private sector to engage in ISE-related policy, governance, planning, and operational coordination, as well as a forum for identifying and satisfying information requirements.

Particularly critical is the coordination of CI/KR information sharing at the national level with that at the local level, where most decisions are made and actions taken to support CI/KR protection. The implementation of the ISE and the formation of the State, Local, and Tribal Government Coordinating Council as a key component of the Sector Partnership are critical to this necessary coordination. Consequently, the integration of the CI/KR information sharing framework into the ISE as its private-sector component strengthens the foundation for effective coordination.

In addition, OIP works closely with and supports Assistant Secretary Charles Allen and OIA in DHS's efforts to use and integrate into State and Local Fusion Centers. The OIP exchanges information with the Fusion Centers using existing channels such as the NICC and HITRAC.

Sustainable Information Sharing

The foundation for sustainability of CI/KR information sharing comes from leveraging the structures, processes, and mechanisms for responding to natural disasters and accidents. When there is a terrorist incident, the tools will already be in place, the training will be complete, and the familiarity and experience required to efficiently implement defined procedures will already be established.

The NICC has undertaken a comprehensive effort to identify relevant and useful all-hazards information available from agencies within DHS to populate CI/KR portals on HSIN-CS. The NICC is the DHS CI/KR hub to ensure that DHS-sourced information remains current. Additionally, OIP has undertaken a project to generate various operational products for CI/KR derived from resources freely available in the public domain. These will include specific products requiring open source research and analysis, as well as a currently available daily reports.

The sectors themselves determine appropriate and useful content for their sector. Some of the SSAs produce sector-specific, non-terrorism related informational products that other sectors find useful for situational awareness and management of incidents related to their CI/KR. Both public and private partners within the sector work with DHS to identify the functional and security capabilities to enable the storage and management of their information on HSIN-CS, as appropriate.

Measurement of Effective Information Sharing

The goals for information sharing in the CI/KR environment are effective and efficient protection, preparedness, response, and mitigation of consequences to incidents that could disrupt the nation's CI/KR. The Sector Partnership represents the foundation for these activities and the information sharing that supports them. Change is a constant: the threat evolves; industries evolve, and the environment within which businesses must operate and provide services and products to the nation evolves. Information requirements will change accordingly. Successful information sharing is measured by the outcomes associated with protection, the efficiency and effectiveness of actions taken, and the adaptability of the entire structure of the Sector Partnership and its supporting information-sharing mechanisms.

With a clear focus on the desired outcomes of protection, and a foundation for systematic engagement and relationships based on trust, an information-sharing environment for CI/KR can sustain itself, adapt, and protect the nation's CI/KR and its citizens.

In closing, I would like to assure you that DHS is relentless in its work to continue building a strong, positive partnership with the private sector in which valuable, actionable information can be shared with the right people at the right time to ensure the protection of our nation's most valuable CI/KR. Our country deserves nothing less. I thank you for your time and appreciate the opportunity to answer any questions you may have.